OFFICE OF THE GOVERNOR

CHIEF PROCUREMENT OFFICE
GENERAL SERVICES

MEMORANDUM

TO: Agency Chief Information Officers
State Purchasing Officers
Agency Procurement Staff
CMS Bureau of Strategic Sourcing
CMS Bureau of Communication and Computer Services

CC: Procurement Policy Board
Procurement Compliance Monitors
Ryan Croke, Chief of Staff, Office of the Governor

FROM: Sean Vinck, State Chief Information Officer
Matt Brown, Chief Procurement Officer for General Services

DATE: August 12, 2014

RE: Review of Information Technology ("IT") Procurements for Compliance with Open Operating Standards Act

---

The purpose of this memorandum is to advise State personnel that the Open Operating Standards Act ("Act"), 20 ILCS 45/1 *et seq.*, became law on March 19, 2014 upon approval by Governor Quinn and is now effective. The Act has a number of implications for State operations. This memorandum, focusing on the technology and procurement implications of the law, articulates a method of validating compliance with the new law while avoiding adding significant complexity or time to existing procedures.

Section 15(g) of the Act requires that cloud computing options be evaluated and, if possible and feasible, adopted for IT procurements. Specifically, that Section provides:

> Consistent with both the Executive Order 10 (2010) directive requiring State agencies to limit information technology expenditures by increasing the use of cloud computing where appropriate, and with the initiatives and standards announced in the United States Department of Homeland Security publication "Federal Cloud Computing Strategy" dated February 8, 2011, *all State agencies are required to evaluate safe, secure cloud computing options, before making any new information technology or telecommunications investments, and, if feasible, adopt appropriate cloud computing solutions*. Each State agency shall re-evaluate its technology sourcing strategy to include consideration and use of cloud computing solutions as part of the budget process.

20 ILCS 45/15(g) (emphasis added).

In accordance with Section 15(g), for all future IT investments – including competitive procurements (RFP, IFB), quasi-competitive or non-competitive acquisitions (sole source, economically feasible sole source, emergency, small purchase) or purchase transactions (orders off master, contract amendments, and change orders) – the procuring agency must demonstrate that it has conducted an examination of the feasibility of employing a cloud solution. If the agency seeks a non-cloud solution, it must provide a rationale for why adopting a cloud-based approach is not feasible.

To confirm compliance with the cloud policy set forth in the Open Operating Standards Act, an agency must submit to the SPO a copy of the attached checklist.

In cooperation with the State CIO, the CPO-GS is directing SPOs to work with their agency counterparts to validate that agencies have considered the requirements of the Act prior to issuing a solicitation for IT services or supports. For such solicitations, agencies will be asked to briefly describe the efforts and conclusions of their review process before the SPO will approve the solicitation method.

Agencies should confirm with the SPO that the IT procurement complies with the NIST definition of cloud computing as explained below. In any situation where a disagreement exists over whether or to what extent the Act applies, the SPO or CPO, as appropriate, will work with the State CIO to resolve the issue.

The NIST Definition of Cloud Computing

The Open Operating Standards Act defines "cloud computing" as "having the meaning provided by Special Publication 800-145 issued by the National Institute of Standards and Technology ["NIST"] of the United States Department of Commerce." NIST defines "cloud computing" as:

> [A] model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.*, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

In order to fit the NIST definition, the technology in question must exhibit (i) each of the five essential characteristics, (ii) fall within one of the four deployment models, or (iii) deliver one of the three service models.

1. The Five Essential Characteristics of Cloud Computing

NIST Special Publication (NIST SP) 800-145 at 2. Per NIST's guidelines, cloud computing has five essential characteristics:

1. On-demand self-service;
2. Broad network access;
3. Resource pooling;

4. Rapid elasticity; and
5. Measured service.

In order to make the determination of whether a proposed IT investment meets the test of the Act, agencies should address each of the following questions which correspond to the five essential characteristics and are based on the definitions in NIST SP 800-145.

1. Does the model in question enable a consumer to unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider?

2. Do capabilities that are available over the network and accessible through standard mechanisms promote use by heterogeneous thin or thick client platforms (*e.g.*, mobile phones, tablets, laptops, and workstations)?

3. Are the provider's computing resources (storage, processing, memory, and network bandwidth) pooled so as to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand, and to give consumers a sense of location independence in that the customer has little or no knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction?

4. Can capabilities be elastically provisioned and released, at least in some cases automatically, to scale rapidly outward and inward commensurate with demand, such that the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time?

5. Does the deployment model in question automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (*e.g.*, storage, processing, bandwidth, and active user accounts) in a way that can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service?

Each of the foregoing questions must be answered in the affirmative. If the answer to any one of the questions is "no", the deployment model in question does not meet all of the definition's essential characteristics and therefore would not comply with Illinois law.

Since it is difficult for the State, using current resources, to deploy models that exhibit each of the five essential characteristics, the Act's preference for cloud computing solutions will prompt serious consideration of other delivery models (as opposed to a "private cloud" model) in the coming months and years.

2. The Four Delivery Models

There are four cloud deployment models. The infrastructure of a *private cloud* "is provisioned for exclusive use by a single organization comprising multiple consumers", such as business units. NIST SP 800-145 at 3. A private cloud "may be owned, managed, and operated by the organization, a third party, or some combination" thereof. *Id.* A private cloud may exist on or off the premises of the organization.

The *community cloud* infrastructure "is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (*e.g.* mission, security requirements, policy, and compliance considerations)." *Id.* A community cloud "may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them." *Id.* It may exist on or off premises." *Id.*

The infrastructure of the *public cloud* is "provisioned for open use by the general public. *Id.* A public cloud "may be owned, managed, and operated by a business, academic, or government organization, or some combination of them." *Id.* It exists on the premises of the cloud provider.

The infrastructure of a *hybrid cloud* is "a composition of two or more distinct cloud infrastructure (private, community, or public) that remain unique entities, but are bound together by standardized or propriety technology that enables data and application portability (*e.g.*, cloud bursting for load balancing between clouds)." *Id.*

3. The Three Service Models

In order to fall within the statutory definition, the technology in question must fall within one of the three services models – Infrastructure-as-a-Service (IAAS), Platform-as-a-service (PAAS), or Software-as-a-service (SAAS.)

For *IAAS*, "the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications." NIST SP 800-145 at 3. Furthermore, "the consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)." *Id.*

For *PAAS*, the consumer is provided "the capability to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider." *Id.* at 2-3. Although consumers do not "manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage," they have "control over the deployed applications and possibly configuration settings for the application-hosting environment." *Id.* at 3.

For *SAAS*, "[t]he capability provided to the consumer is to use the provider's applications running on a cloud infrastructure." *Id.* at 2. A "cloud infrastructure" is defined as "is the collection of hardware and software that enables the five essential characteristics of cloud computing." *Id.* at 2, fn.2.